IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA	CRIMINAL NO. 1:13-CR-341
v.	Count 1: 18 U.S.C. § 1030(a)(5)(A) Intentionally Causing Damage To A Protected Computer
JONATHAN HARTWELL WOLBERG,	
Defendant.	Counts 2-18: 18 U.S.C. § 1030(a)(5)(B) Recklessly Causing Damage To A Protected Computer
	Count 19: 18 U.S.C. § 1028A(a)(1) Aggravated Identity Theft
	Forfeiture Notice

INDICTMENT

THE GRAND JURY CHARGES THAT:

GENERAL ALLEGATIONS

At all times relevant to the Indictment:

1. From on or about March 16, 2012 until on or about August 1, 2012, the defendant, JONATHAN HARTWELL WOLBERG, without authorization, repeatedly entered the networks and computers of Company A, his former employer, for the purpose of damaging Company A and its business. In the process, WOLBERG caused loss and damage to Company A and its customers, and caused potential modification and impairment of patient medical care.

2. Company A, known to the grand jury, was a corporation headquartered in the Eastern District of Virginia, and provided Internet-based computing and storage ("cloud-computing") services, some of which were also located in the Eastern District of Virginia.

Customers, including medical care facilities servicing hospitals, used Company A's services for stable, reliable, and real-time access to information on its servers.

3. Defendant JONATHAN HARTWELL WOLBERG worked as a systems administrator for Company A, first in Virginia and later in Arizona, where he worked remotely. WOLBERG was responsible for building and operating Company A's networks and servers. WOLBERG resigned from Company A on or about February 15, 2012.

WOLBERG Repeatedly Logs Into Company A's Systems Without Authorization

4. After defendant JONATHAN HARTWELL WOLBERG resigned from Company A, he repeatedly logged into Company A's systems in the Eastern District of Virginia from his home computer in Tucson, Arizona and deleted data, turned off and disabled servers, and otherwise interfered with Company A's systems. To hide his unauthorized accesses to Company A's internal network, he logged in indirectly through other computers first.

5. In this way, defendant JONATHAN HARTWELL WOLBERG routinely accessed sensitive internal documentation of Company A's computer systems, including administrative usernames and passwords, computer names, information about Company A's software and hardware, and information about Company A's computer vulnerabilities. WOLBERG also downloaded internal web pages describing Company A's web servers and its client lists.

6. While engaging in unauthorized accesses, defendant JONATHAN HARTWELL WOLBERG encouraged other Company A customers to leave. For example:

a. On or about February 15, 2012, WOLBERG emailed a customer to state about Company A: "I don't think they are very long for this world."

b. On or about February 21, 2012, WOLBERG sent chat messages to a former colleague at Company A, stating: "I know you got 50 things going n like usual, but dont forget to get me your partner Id and registered company name for my cents . . . Sooner I can pull that from [Company A] to knock em down a peg th e better[.]"

c. On or about April 4, 2012, WOLBERG emailed a customer of Company A, stating: "As you were made aware, I recently left [Company A] to pursue other opportunities right in the middle of finalizing the purchase of their array. I want to apologize for the unfortunate experience you had while working with [Company A] after I left. Hopefully things have stabilized there for you." WOLBERG then introduced a competitor of Company A to the customer.

d. On or about May 3, 2012, WOLBERG emailed a customer of Company A, stating: "I just wanted to drop you a line and let you know that the Equinix/[Company A] relationship isn't on the best of terms right now. If you are looking to do Amsterdam I can hook you up with someone direct at Equinix who can give you much more aggressive rates."

e. On or about May 15, 2012, WOLBERG sent chat messages to a customer of Company A, stating: "well, no one [at Company A] has been updating anything for 4+ months . . . You guys looking at moving elsewhere or going to stay for the long term?"

f. On or about May 30, 2012, WOLBERG sent an email to a customer of Company A, introducing the customer to a competitor of Company A.

g. On or about June 6, 2012, WOLBERG sent chat messages to a customer of Company A, stating: "so have you made any progress on your shopping? . . . who else are you looking at since we talked last? . . . im just a bit surprised that [Company A] arent addressing

your concerns like they should be . . . well, at least you wont be the only customer leaving . . . other private cloud customers are leaving in droves too[.]"

h. On or about June 7, 2012, WOLBERG sent an email to a customer of Company A, introducing the customer to a competitor of Company A and stating: "I wouldn't expect [Company A] to be able to do anything complex for you like hardware quotes or advice on what to buy, etc. They have no one left technical enough to do that ([another person] did it in my place but he doesn't know as much about [hardware] as I do). . . . You aren't the only customer having issues though, lots of the private cloud customers have already left or are in the process of leaving due to lack of support, basic items taking days, outages for dumb stuff like licenses expiring, etc."

7. On or about June 23, 2012, at approximately 1:58 A.M., defendant JONATHAN HARTWELL WOLBERG logged into a server used by Company A. Over the next half hour, WOLBERG searched Google for "esxi power off all VMs" to learn how to turn off software used by Company A to provide services to its customers. WOLBERG also searched Google for "how to clear RDP history" to learn how to conceal his remote logins into Company A's systems.

8. On or about June 25, 2012, starting at approximately 12:53 A.M, defendant JONATHAN HARTWELL WOLBERG again searched for information about how to turn off software that was providing services to Company A's customers. For example, WOLBERG searched Google for "esxi how to manually power off VM," "esxi clear bash history," "esxi clear command line history," and "linux how to empty running file" to do so. "Esxi" is a type of software that operates Company A's "cloud-computing" systems.

9. Also on or about June 25, 2012, defendant JONATHAN HARTWELL WOLBERG convinced an employee of Company A, Person A, to provide him with Person A's username and password into Company A's internal network. WOLBERG told Person A he was looking for old documents that WOLBERG had drafted while still at Company A.

10. To obtain Person A's username and password, defendant JONATHAN HARTWELL WOLBERG stated: "i have access to stuff they dont know about that will just show it being logged in from the backend network . . . so it wont show anything . . . if they actually read through the logs, it'd show me logging in from the office[.]"

11. In reality, defendant JONATHAN HARTWELL WOLBERG used Person A's username and password to search for ways to shut down Company A's servers. Between approximately 8:48 P.M. and 9:22 P.M., WOLBERG copied several of Company A's internal documentation files to his computer's hard drive to review for information about Company A's servers.

12. For the next several hours, defendant JONATHAN HARTWELL WOLBERG reviewed the items he had downloaded from Company A and researched additional information about how to bring down Company A's servers. For example, WOLBERG searched Google for "vnx how to delete component LUN," "how to shutdown SP," and "VNX how to shutdown." VNX is a type of server belonging to Company A.

13. At about 12:42 A.M. on June 26, 2012, defendant JONATHAN HARTWELL WOLBERG reviewed a document entitled "VNX 5300 Unified power off procedure.pdf" and searched Google for "windows 2003 disable security event logging" to learn about how to conceal his activities.

WOLBERG Damages Company A's Computer Systems

14. On the evening of June 27, 2012, defendant JONATHAN HARTWELL WOLBERG visited several web pages containing instructions about how to turn off Company A's storage server and again reviewed the document entitled "VNX 5300 Unified power off procedure.pdf," including at about 9:09 P.M. This document included instructions on a command called "nas_halt" which would shut down a VNX server owned and operated by Company A.

15. At approximately 9:13 P.M., defendant JONATHAN HARTWELLWOLBERG logged into Company A's storage server and issued the "nas_halt" command, shutting it down.

16. When defendant JONATHAN HARTWELL WOLBERG shut down Company A's server, customers, including Company B, a health care information technology client providing services to hospitals, were denied access to their records, including records for patient care.

17. Within an hour of using the "nas_halt" command, defendant JONATHAN HARTWELL WOLBERG visited the websites of Company A's customers, including that of Company B and that of two other customers, to confirm that his attack had succeeded.

18. On or about July 11, 2012, defendant JONATHAN HARTWELL WOLBERG received a chat message from a former colleague at Company A, stating: "i just hope no one that left was stupid enough to do anything because that would be a felony . . . ." WOLBERG responded: "true, but they wont find anything . . . oh yea huge felony[.]"

19. Also on or about July 11, 2012, defendant JONATHAN HARTWELL WOLBERG sent a chat message to a former colleague at Company A, stating: "so ever if they did catch that log of me jumping into something, there was nothing to show i actually did

anything. They could come after me for being an unauthorized user in a system, but the fault lies with them for not changing passwords."

20. On or about July 13, 2012, defendant JONATHAN HARTWELL WOLBERG engaged in a chat message with a former colleague at Company A. The former colleague warned about the FBI's involvement, to which WOLBERG responded: "yea i wouldnt worry too much about that man, even if they could find something, you can claim you were hacked, and your password isnt following the company secure password policy anyway[.]"

21. As a result of defendant JONATHAN HARTWELL WOLBERG's intrusions, Company A and its customers suffered losses aggregating at least $5,000 during a 1-year period.

COUNT ONE

(Intentionally Causing Damage To A Protected Computer)

THE GRAND JURY FURTHER CHARGES:

22. Paragraphs 1 through 21 are re-alleged and incorporated by reference.

23. On or about June 27, 2012, within the Eastern District of Virginia and elsewhere, defendant JONATHAN HARTWELL WOLBERG knowingly caused the transmission of information, code, and command, and attempted to do so, and, as a result of such conduct, intentionally caused damage without authorization to a protected computer, causing loss during a 1-year period from the defendant's course of conduct affecting protected computers aggregating at least $5,000 in value, and causing the potential modification and impairment of the medical examination, diagnosis, treatment, and care of individuals.

(In violation of Title 18, United States Code, Sections 1030(a)(5)(A) and (c)(4)(A)(i)(I)-(II), (c)(4)(B)(i).)

COUNTS TWO THROUGH EIGHTEEN

(Recklessly Causing Damage To A Protected Computer)

THE GRAND JURY FURTHER CHARGES:

24. Paragraphs 1 through 21 are re-alleged and incorporated by reference.

25. On or about the following dates, each date constituting a separate count, within the Eastern District of Virginia and elsewhere, defendant JONATHAN HARTWELL WOLBERG intentionally accessed a protected computer without authorization, and attempted to do so, and as a result of such conduct, recklessly caused damage, causing loss to 1 and more persons during a 1-year period, including loss resulting from a related course of conduct affecting one and more protected computers, and aggregating at least $5,000 in value, and causing the potential modification and impairment of the medical examination, diagnosis, treatment, and care of individuals:

Count	Date	Access
2	3/18/2012	Access from computer REANNA
3	4/3/2012	Access from computer REANNA
4	4/9/2012	Access from computer JONWOLBERG-PC
5	4/10/2012	Access from computer JONWOLBERG-PC
6	4/11/2012	Access from computer JONWOLBERG-PC
7	4/12/2012	Access from computer JONWOLBERG-PC
8	4/15/2012	Access from computer JONWOLBERG-PC
9	4/24/2012	Access from computer JONWOLBERG-PC
10	4/26/2012	Access from computer JONWOLBERG-PC
11	5/4/2012	Access from computer JONWOLBERG-PC
12	6/21/2012	Access from computer JONWOLBERG-PC
13	6/23/2012	Access from computer JONWOLBERG-PC
14	6/25/2012	Access from computer JONWOLBERG-PC
15	6/26/2012	Access from computer JONWOLBERG-PC
16	6/27/2012	Access from computer JONWOLBERG-PC
17	6/28/2012	Access from computer JONWOLBERG-PC
18	6/29/2012	Access from computer JONWOLBERG-PC

(In violation of Title 18, United States Code, Sections 1030(a)(5)(B) and 1030(c)(4)(A)(i)(I)-(II).)

COUNT NINETEEN

(Aggravated Identity Theft)

THE GRAND JURY FURTHER CHARGES:

26. Paragraphs 1 through 21 are re-alleged and incorporated by reference.

27. On or about June 25, 2013, within the Eastern District of Virginia and elsewhere, defendant JONATHAN HARTWELL WOLBERG did knowingly transfer, possess, and use, without lawful authority, a means of identification of another person during and in relation to felonies enumerated in 18 U.S.C. § 1028A(c), to wit: Intentionally Causing Damage To A Protected Computer, in violation of 18 U.S.C. §§ 1030(a)(5)(A) and 1030(c)(4)(B)(i), and Recklessly Causing Damage To A Protected Computer, in violation of 18 U.S.C. §§ 1030(a)(5)(B) and 1030(c)(4)(A)(i)(I)-(II).

(In violation of Title 18, United States Code, Sections 1028A(a)(1), 1030(a)(5)(C) and (c)(4)(G).)

NOTICE OF FORFEITURE

Pursuant to Federal Rule of Criminal Procedure 32.2(a), the defendant is hereby notified that upon conviction of the offenses in violation of Title 18, United States Code, Section 1030 set forth in Counts 1 through 18 of this Indictment, defendant JONATHAN HARTWELL WOLBERG, shall forfeit to the United States of America, pursuant to Title 18, United States Code. Sections 982(a)(2)(B) and 1030(i)(1)(B), any property constituting, or derived from, proceeds obtained, directly or indirectly, as a result of such violations; and pursuant to Title 18, United States Code, Section 1030(i)(1)(A), any personal property used or intended to be used to commit the offenses. If any of the property described above as being forfeitable pursuant to Title 18, United States Code, Sections 982(a)(2)(B) and 1030(i), as a result of any act or omission of the defendant:

a. cannot be located upon the exercise of due diligence;

b. has been transferred or sold to, or deposited with, a third party;

c. has been placed beyond the jurisdiction of the court;

d. has been substantially diminished in value; or

e. has been commingled with other property which cannot be divided without difficulty;

It is the intention of the United States of America, pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Section 982(b)(1), and Title 18, United States Code, Section 1030(i)(2), to seek forfeiture of all other property of the defendant up to the value of the property described above.

(All pursuant to 18 U.S.C. §§ 982(a)(2)(B) and 1030(i).)

A TRUE BILL:

Pursuant to the E-Government Act, the original of this page has been filed under seal in the Clerk's Office.

_____
Foreperson of the Grand Jury

NEIL H. MACBRIDE
UNITED STATES ATTORNEY

By: _____
Jonathan Keim
Special Assistant United States Attorney (LT)
Alexander T.H. Nguyen
Assistant United States Attorney